UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/542,630	04/24/2006	Christian Benardeau	0512-1290	1731

466 7590 12/31/2008
YOUNG & THOMPSON
209 Madison Street
Suite 500
ALEXANDRIA, VA 22314

EXAMINER	
ARCHER, CHRISTOPHER B	

ART UNIT	PAPER NUMBER
4148	

MAIL DATE	DELIVERY MODE
12/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/542,630	BENARDEAU, CHRISTIAN	
	Examiner	Art Unit	
	CHRISTOPHER B. ARCHER	4148	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 April 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-20* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-20* is/are rejected.

7)☒ Claim(s) *5-8 and 19* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *18 July 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *07/18/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. The instant application having Application No. 10/542,630 filed on 07/18/2005 is presented for examination by the examiner.

Oath/Declaration

2. The applicant's oath/declaration has been reviewed by the examiner and is found to conform to the requirements prescribed in **37 C.F.R. 1.63**.

Priority

3. As required by **M.P.E.P. 201.14(c)**, acknowledgement is made of applicant's claim for priority based on applications filed on 01/17/2003 (FR 03/00525).

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Examiner Notes

4. Examiner cites particular columns and line numbers in the references as applied to the claims below for the convenience of the applicant. Although the specified citations are representative of the teachings in the art and are applied to the specific limitations within the individual claim, other passages and figures may apply as well. It is respectfully requested that, in preparing responses, the applicant fully consider the references in entirety as potentially teaching all or part of the claimed invention, as well as the context of the passage as taught by the prior art or disclosed by the examiner.

Specification

5. The following guidelines illustrate the preferred layout for the specification of a utility application. These guidelines are suggested for the applicant's use.

Arrangement of the Specification

As provided in 37 CFR 1.77(b), the specification of a utility application should include the following sections in order. Each of the lettered items should appear in upper case, without underlining or bold type, as a section heading. If no text follows the section heading, the phrase "Not Applicable" should follow the section heading:

(a) TITLE OF THE INVENTION.
(b) CROSS-REFERENCE TO RELATED APPLICATIONS.
(c) STATEMENT REGARDING FEDERALLY SPONSORED RESEARCH OR DEVELOPMENT.
(d) THE NAMES OF THE PARTIES TO A JOINT RESEARCH AGREEMENT.
(e) INCORPORATION-BY-REFERENCE OF MATERIAL SUBMITTED ON A COMPACT DISC.
(f) BACKGROUND OF THE INVENTION.
    (1) Field of the Invention.
    (2) Description of Related Art including information disclosed under 37 CFR 1.97 and 1.98.
(g) BRIEF SUMMARY OF THE INVENTION.
(h) BRIEF DESCRIPTION OF THE SEVERAL VIEWS OF THE DRAWING(S).
(i) DETAILED DESCRIPTION OF THE INVENTION.
(j) CLAIM OR CLAIMS (commencing on a separate sheet).
(k) ABSTRACT OF THE DISCLOSURE (commencing on a separate sheet).
(l) SEQUENCE LISTING (See MPEP § 2424 and 37 CFR 1.821-1.825. A "Sequence Listing" is required on paper if the application discloses a nucleotide or amino acid sequence as defined in 37 CFR 1.821(a) and if the required "Sequence Listing" is not submitted as an electronic document on compact disc).

Claim Rejections - 35 USC § 101

6. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

Claims 10 and 11 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter because of the following reason:

The claims fail to place the invention squarely within one statutory class of invention. The applicant has failed to provide evidence that applicant does not intend the "medium" to include signals. As such, the claim is drawn to a form of energy. Energy is not one of the four categories of invention and therefore this claim(s) is/are not statutory. Energy is not a series of steps or acts and thus is not a process. Energy is not a physical article or object and as such is not a machine or manufacture. Energy is not a combination of substances and therefore not a composition of matter.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

8. Claims 1-5, 9-11, 15-17, and 19 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard, et al. (U.S. Pub. No. 2002/0129249 A1), hereafter referred to as Maillard, in view of Booth, et al. (WO 01/61437 A2).

Regarding claim 1:

Maillard discloses "Method for ensuring the integrity of at least one computer software program which can be carried out by means of at least one encryption/decryption module, the at least one computer software program being

transmitted, by means of a transmitter, to a decoder which is equipped with the at least one encryption/decryption module by means of a long-distance information transmission network, the transmitter carrying out:

a) a step (40) for encrypting information signals transmitted to the decoder, **[(Maillard [0102]) shows the transmitter encrypting broadcast information.]**

b) a step (50) for transmitting, to the at least one encryption/decryption module of the decoder, a message containing the information required for the decoder to decrypt the information signals transmitted at step a), **[(Maillard [0097], [0099]) shows the generation and transmission of a control word. The control word is necessary for the decryption of the encrypted information.]** and

c) a step (42, 100) for transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder **[(Maillard [0101]-[0104]) shows the scrambled information being sent from the transmitter to the end user's receiver/decoder.]**"

But Maillard fails to explicitly disclose

"the decoder carrying out:

d) a step (74) for decrypting the information signals transmitted by the transmitter during step a) using the information provided for this purpose in the message transmitted during step b), characterised:

- in that the transmitter inserts (at 52, 124) in the message transmitted during step b) an additional item of information which allows the at least one

encryption/decryption module to verify that it has effectively received the or each computer software program transmitted at step c),

- in that the at least one encryption/decryption module verifies (at 60), based on the additional information inserted by the transmitter in the message transmitted during step b), whether it has effectively received the or each software program transmitted during step c), and
- in that, if the or each software program has not been received, the at least one encryption/decryption module prevents step d) (at 68)."

However, Booth discloses:

"the decoder carrying out:

d) a step (74) for decrypting the information signals transmitted by the transmitter during step a) using the information provided for this purpose in the message transmitted during step b), characterised:

- in that the transmitter inserts (at 52, 124) in the message transmitted during step b) an additional item of information which allows the at least one encryption/decryption module to verify that it has effectively received the or each computer software program transmitted at step c),
- in that the at least one encryption/decryption module verifies (at 60), based on the additional information inserted by the transmitter in the message transmitted during step b), whether it has effectively received the or each software program transmitted during step c), and

- in that, if the or each software program has not been received, the at least one encryption/decryption module prevents step d) (at 68)."

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

Maillard and Booth are analogous art because they are from the same field of endeavor of broadcast information security.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Maillard to prevent the usage of information found to be incomplete or inaccurate, as found in the teaching of Booth, in order to prevent the corruption of received data.

Regarding claim 2:

Maillard further discloses "Method according to claim 1, characterised in that the transmitter encrypts (at 50) the message transmitted at step b), and in that the at least one encryption/decryption module decrypts the message transmitted during step b) in order to allow step d) to be carried out" as

[(Maillard [0097], [0099]) shows a system that encrypts a control word necessary to decrypt the data at the corresponding receiver.]

Regarding claim 3:

Booth further discloses "Method according to claim 1, characterised in that the transmitter carries out:

c) a step (44, 122) for constructing a first identifier of the or each computer software program transmitted during step c), and

f) a step (52, 124) for inserting this identifier in the message transmitted during step b), and in that the at least one encryption/decryption module carries out:

g) a step (62, 110) for reconstructing the identifier of the or each computer software program based on the or each computer software program received,

h) a step (66, 112) for comparing the identifier reconstructed at step g) with the identifier inserted by the transmitter during step f), and

i) if the identifier reconstructed at step g) does not correspond to that inserted at step f) in the message transmitted at step b), a step (68, 108) for preventing step d),

j) if the identifier reconstructed at step g) corresponds to the identifier inserted at step f) in the message transmitted during step b), a step (66, 112) for validating the integrity of the or each computer software program."

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

Regarding claim 4:

Booth further discloses "Method according to claim 3, for ensuring the integrity of a group of several computer software programs which can each be carried out by the at least one encryption/decryption module, characterised in that step e) comprises an operation (44) for constructing a single identifier for the group of several computer software programs to be transmitted during step c) based on information relating to each of the software programs of the group and in that step g) consists in carrying out the same operation as that carried out during step e) in order to reconstruct a unique identifier corresponding to that constructed during step e) if the group received by the decoder is identical to that transmitted by the transmitter" as

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

Regarding claim 5:

"Method according to claim 3, characterised in that the steps d), g), h), i) and j) are carried out by the same encryption/decryption module."

[(Booth page 6, lines 22-26) shows a single secure processor for carrying out the various security authentications.]

Regarding claim 9:

Booth further discloses "Method according to claim 2, characterised in that the at least one encryption/decryption module carries out the at least one computer software program each time the integrity thereof is validated during step j)" as

[(Booth page 17, lines 18-30) shows that the master processor can access or execute authenticated sections of code as needed.]

Regarding claim 10:

Maillard further discloses "Information recording medium (12) comprising instructions for carrying out a method according to claim 1, when the instructions are carried out by the transmitter (4)" as

[(Maillard [0091], [0092] and Figure 2) shows a "mother" smartcard connected to the ciphering units. The mother smartcard controls the operations of the ciphering unit.]

Regarding claim 11:

Maillard further discloses "Information recording medium (22, 88) comprising instructions for carrying out a method according to claim 1, when the instructions are to be carried out by the at least one encryption/decryption module" as

[(Maillard [0091], [0092] and Figure 2) shows a "daughter" smartcard connected to the receiver/decoder units. The daughter smartcard controls the operations of the receiver/decoder unit.]

Regarding claim 15:

Maillard further discloses "Transmitter (4) which is suitable for carrying out a method according to claim 1, this transmitter (4) being capable of:

- encrypting information signals transmitted to the or each decoder, **[(Maillard [0102]) shows the transmitter encrypting broadcast information.]**
- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and **[(Maillard [0097], [0099]) shows the generation and transmission of a control word. The control word is necessary for the decryption of the encrypted information.]**
- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder, characterised: **[(Maillard [0101]-[0104]) shows the scrambled information being sent from the transmitter to the end user's receiver/decoder.]**
- in that the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted **[(Maillard [0231]) shows that the system can include a checksum for the purposes of data integrity.]**"

Regarding claim 16:

Booth further discloses "Decoder (6, 82) which is suitable for carrying out a method according to claim 1, this decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter, and being equipped with the at least one encryption/decryption module (16, 84);

characterised:

- in that the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and
- in that, if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted" as

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

Regarding claim 17:

Maillard further discloses "Decoder (6, 82) according to claim 16, characterised in that it is equipped with a single removable encryption/decryption module" as

[(Maillard [0106]) shows a "daughter" smartcard that slots into a housing in the receiver/decoder.]

Regarding claim 19:

Booth further discloses "Method according to claim 2, characterised in that the transmitter carries out:

e) a step (44, 122) for constructing a first identifier of the or each computer software program transmitted during step c), and

f) a step (52, 124) for inserting this identifier in the message transmitted during step b), and in that the at least one encryption/decryption module carries out:

g) a step (62, 110) for reconstructing the identifier of the or each computer software program based on the or each computer software program received,

h) a step (66, 112) for comparing the identifier reconstructed at step g) with the identifier inserted by the transmitter during step f), and

i) if the identifier reconstructed at step g) does not correspond to that inserted at step f) in the message transmitted at step b), a step (68, 108) for preventing step d),

j) if the identifier reconstructed at step g) corresponds to the identifier inserted at step f) in the message transmitted during step b), a step (66, 112) for validating the integrity of the or each computer software program."

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

9. Claims 12 and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Booth.

Regarding claim 12:

Maillard discloses "System for ensuring the integrity of at least one computer software program which can be carried out by at least one encryption/decryption module (16, 84), the system comprising a transmitter (4) for transmitting the at least one computer software program via a long-distance information transmission network (8), and a decoder (6, 82) which is equipped with the at least one encryption/decryption module (16, 84),

the transmitter (4) being capable of:

- encrypting information signals transmitted to the or each decoder, **[(Maillard [0102]) shows the transmitter encrypting broadcast information.]**
- transmitting to the at least one encryption/decryption module of the decoder a message containing the information required for the decoder to decrypt the information signals transmitted, and **[(Maillard [0097], [0099]) shows the**

generation and transmission of a control word. The control word is necessary for the decryption of the encrypted information.]

- transmitting the at least one computer software program to the at least one encryption/decryption module of the decoder, the decoder (6, 82) being capable of decrypting the information signals transmitted by the transmitter using the information which is provided for this purpose and which is contained in the message transmitted by the transmitter **[(Maillard [0101]-[0104]) shows the scrambled information being sent from the transmitter to the end user's receiver/decoder.],**

But, Maillard fails to disclose

"characterised:

- in that the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted,
- in that the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and
- in that, if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted."

However, Booth discloses

"characterised:

- in that the transmitter (4) is capable of inserting in the message an additional item of information which allows the at least one encryption/decryption module (46, 84) to verify that it has received the or each computer software program transmitted,
- in that the at least one encryption/decryption module (16, 84) is capable of verifying, based on the additional information inserted by the transmitter in the message, whether it has effectively received the or each software program transmitted by the transmitter, and
- in that, if the or each software program has not been received, the at least one encryption/decryption module (16, 84) is capable of preventing the decryption of the information signals transmitted."

[(Booth page 6, lines 12-31) shows a computer system that receives blocks of code. Each block was sent with an "authentication signature". The computer system then checks the sent authentication signature against an associated value that it computes from the transmitted block of code. If the two values fail to match, the computer purges the unauthenticated block of code.]

Maillard and Booth are analogous art because they are from the same field of endeavor of broadcast information security.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the teachings of Maillard to prevent the usage of information found

to be incomplete or inaccurate, as found in the teaching of Booth, in order to prevent the corruption of received data.

Regarding claim 13:

Maillard further discloses "System according to claim 12, characterised in that the or each decoder (6) is equipped with a single removable encryption/decryption module" as **[(Maillard [0106]) shows a "daughter" that slots into a housing in the receiver/decoder.]**

10. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Booth and further in view of Gammie (U.S. Patent No 5,029,207), hereafter referred to as Gammie.

Regarding claim 18:

Maillard and Booth disclose "Decoder (6, 82) according to claim 16," but fail to explicitly disclose "characterised in that it is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder."

However, Gammie discloses "characterised in that it is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder" as

[(Gammie column 10, lines 4-10 and Figure 7) shows a decryption module with both an internal and external security device. The external security device is removable.]

Gammie and Maillard are analogous art because they are from the same field of endeavor of security modules for broadcast encryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Maillard to use both internal and external security modules for increased piracy protection as described in Gammie. An internal security module provides protection against physical alteration of the decoder/receiver and an external module allows for easy security upgrades and termination of compromised modules.

11. Claim 14 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Booth and further in view of Gammie.

Regarding claim 14:

Maillard and Booth disclose "System according to claim 12," but fail to explicitly disclose "characterised in that the or each decoder (82) is equipped with at least two autonomous encryption/decryption modules which are independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder."

However, Gammie discloses "characterised in that the or each decoder (82) is equipped with at least two autonomous encryption/decryption modules which are

independent from each other, at least one of these encryption/decryption modules being fixedly joined to the body of the decoder" as

[(Gammie column 10, lines 4-10) shows a decryption module with both an internal and external security device. The external security device is removable.]

Gammie and Maillard are analogous art because they are from the same field of endeavor of security modules for broadcast encryption.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Maillard to use both internal and external security modules for increased piracy protection as described in Gammie. An internal security module provides protection against physical alteration of the decoder/receiver and an external module allows for easy security upgrades and termination of compromised modules.

12. Claims 6-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Booth and further in view of Nagae (U.S. Patent No. 5,598,530), hereafter referred to as Nagae.

Regarding claim 6:

Maillard and Booth disclose "Method according to claim 3," but fail to explicitly disclose "characterised in that a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g)."

However, Nagae discloses "characterised in that a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g)."

[(Nagae column 3, lines 16-37 and Figure 1) shows a system where a calculating unit calculates a checksum, then a separate control unit compares the checksum with an already stored checksum value. The control unit executes the program if the comparison is positive, and inhibits and deletes the data if the comparison is negative.]

Nagae and Booth are analogous art because they are from the same field of endeavor of data integrity validation.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Booth to include a separate unit used solely for computing a checksum, as described in Nagae, as it reduces the amount of calculations performed by each unit and allows each unit to synchronously perform additional tasks while waiting for output from the other.

Regarding claim 7:

Maillard further discloses "Method according to claim 6, characterised in that the transmitter further carries out:

k) a second step (120) for constructing a second identifier of the or each computer software program transmitted during step c), this second identifier being transmitted together with the or each corresponding software program during step c), and

- in that step g) which is carried out by the second encryption/decryption module comprises:

- an operation (102) for reconstructing the second identifier which is transmitted together with the or each software program,

- only if the second reconstructed identifier corresponds to that transmitted together with the or each software program during step c), an operation (110) for reconstructing the first identifier inserted in the message transmitted during step b) and for transmitting this first reconstructed identifier to the first encryption/decryption module so that the first encryption/decryption module can carry out step h)," as

[(Maillard [0041] and [0095]-[0100]) shows control signals being sent to the receiver/decoder that prevent the decoding of the information if the user does not have the proper rights. This process is done in addition to the error checking process.]

Regarding claim 8:

Maillard further discloses "Method according to claim 7, characterised in that the first and the second identifiers are obtained from the same identifier of the or each computer software program by encrypting the same identifier using a different first and second encryption key, respectively," as

[(Maillard [0095]-[0100]) shows that access criteria and control words are sent in one common ECM.]

13. Claim 20 is rejected under 35 U.S.C. 103(a) as being unpatentable over Maillard in view of Booth and further in view of Nagae.

Regarding claim 20:

Maillard and Booth disclose "Method according to claim 4," but fail to explicitly disclose "characterised in that a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g)."

However, Nagae discloses "characterised in that a first autonomous encryption/decryption module carries out only steps d), h), i) and j), and in that a second autonomous encryption/decryption module which is independent from the first encryption/decryption module and which is fixedly joined to the decoder carries out at least step g)" as

[(Nagae column 3, lines 16-37 and Figure 1) shows a system where a calculating unit calculates a checksum, then a separate control unit compares the checksum with an already stored checksum value. The control unit executes the program if the comparison is positive, and inhibits and deletes the data if the comparison is negative.]

Nagae and Booth are analogous art because they are from the same field of endeavor of data integrity validation.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the invention of Booth to include a separate unit used solely for computing a checksum, as described in Nagae, as it reduces the amount of calculations performed by each unit and allows each unit to synchronously perform additional tasks while waiting for output from the other.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to CHRISTOPHER B. ARCHER whose telephone number is (571)270-7308. The examiner can normally be reached on M-F 7:30-5.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Thomas Pham can be reached on (571)272-3689. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/C. B. A./

Examiner, Art Unit 4148

/Thomas K Pham/
Supervisory Patent Examiner, Art Unit 4148